



Frames and MetaFrames
infectionvectors.com
December 2005

Overview

Late December 2005 revealed another attack on graphic rendering systems used by Microsoft Windows, this time the WMF (Windows Meta Frame) viewing process has proven vulnerable. The exploit quickly made the rounds throughout nefarious sites intent on forcibly installing malicious code and requesting victims pay for removal software. The threat has been taken so seriously by many security groups that they are calling for enterprises to install unsupported, third-party patches ahead of Microsoft's release in early January.

Union of the Nefarious

The exploit was first seen on unionseek.com, and has since been removed from that URL. The domain is registered to:

Registrant:
Technology Systems
Jerry Bahrt *****@trts.ca)
122 Millwick Drive (Unit #3)
North York
Ontario, M9l 1Y6
CA
Tel. +416.6269489

Creation Date: 22-May-2005
Expiration Date: 22-May-2006

Within 24 hours of the original posting, the exploit found its way to numerous sites, all of which attempt to force "anti-malware" software onto the victim machine (as of December 29, 2005). There is little doubt that the exploit will be incorporated into a worm, probably of the mass-mailing variety, within a few days.

Certainly, one could understand if an analyst called the "full disclosure" methodology into question: numerous exploit serving points right after public notification and specification of a new vulnerability. However, that is misplaced in the wake of such a release. The explosion of sites serving the malcode is not necessarily the work of public dissemination of the exploit; it is entirely possible that the various servers are all under the same "management" (or that the code was distributed via private back channel communications).

Once executed, the current incarnations of the WMF-exploit-based malware inform the user that their machine has been compromised (which is, in fact, true) and that they need to purchase software to remove the attacker (which is also true, but the solution offered is certainly not the correct one). The software is then downloaded and executed from a remote server. This software eventually asks for personal/credit card information.

Again, the Internet is faced with a very well organized criminal attempt to make money. There are two scenarios (which are not entirely mutually exclusive) that point to this conclusion:

1) The exploit was published by someone unaffiliated with any for-profit attempt. This assumes that the discoverer and publisher of the exploit code are simply working to make any and all vulnerabilities public. If that is the case, then we have witnessed a rather nimble software creation organization lift the code and incorporate it into a global distribution scheme rather quickly (of course, everything on the Internet is a “global distribution” system).

2) The exploit was crafted and published by a criminal group hoping to profit from such discoveries. This would be a true R&D component of a criminal enterprise. Although that gives them much more latitude in incorporating and distributing new code (since they would have had time to work on the roll out), the dedication to investing in research (especially with this type of success) is worrisome.

What It Is

A day after the exploit began surfacing in public warnings, Microsoft issued a security bulletin (no patch at that time). This out-of-cycle bulletin was a rare divergence for the company; however, it came with important information for all Windows users. The exploit is connected to the Picture and Fax Viewer, SHIMGVW.DLL, and is capable of allowing arbitrary remote code execution. CERT.org reports that the flaw may actually be with GDI32.DLL, meaning that future incarnations of the exploit code would not be stopped by simply disabling the Picture and Fax viewer as has been suggested on some security sites. Machines patched with the recently released (November 2005) MS05-053 (896424) Graphics Rendering Engine fix have been noted to be vulnerable.

Recall the vulnerability from October of 2004 (MS04-032) in the graphics rendering of WMF and EMF files. The unchecked buffer described at that time allowed virtually any type of code to be executed on a remote system. The same type of problem exists again in the latest incarnation of the threat. At that time, Microsoft recommended that users read email in plain text if possible. In the security bulletin released 28 December 2005, the company notes that this is still helpful but does not include it as a mitigation step.

What It Can Be

Sometime within the next week, someone with enough inclination and free time will be inspired to give the publicly available exploit code the mobility of a mass mailer. As with

attacks in the past, there exists the flexibility of either attaching the exploit as a file (with any extension, not just WMF) or as a link pointing to a web server. In either case, the propagation will probably be dependent on reaching out to another server and retrieving the engine for delivering more goodies to addresses found on the infected host.

As mentioned, any graphics extension can be used for the file, as Windows will read the header of the file and determine which viewer it wants to use to open the file. This begs the question of system administrators: how long will it be before such attacks spur the blocking of graphics files along with the traditional EXE, PIF, COM, etc. filters?

This may also end up being another log on the fire for disclosure vs. “responsible” disclosure (meaning tell the vendor secretly until a fix is available). That debate is, of course, as resolvable as one about what the best OS is. Focus needs to remain on how to responsibly disseminate investigation and protection data for known threats, no matter how the threats become “known.” Malware authors are remaining nimble, so should security professionals.

“Nimble” doesn’t necessitate installing a patch that comes without support and with the potential to do much more long-term harm than the malware does. Early after the first waves of malware hit the Internet, one of the most talented low-level Windows programmers on the planet, Ilfak Guilfanov, created a patch for the exploit. Guilfanov is the author of IDA. He is more than qualified to write such a patch. However, that does not mean that security organizations calling for everyone to install the patch are acting responsibly.

Before acting on an unpatched vulnerability, consider the actual level of risk for your enterprise. The WMF flaw is widespread, as noted on nearly every website covering this issue it is probably a problem for every Windows machine in circulation. But, so is every email-borne worm on the Internet. All of them. If a user is inclined to click a link or open an attachment, then the organization has had this problem for a long time – and on every single system in the network, not just the Windows boxes. The amount of WMF-based malware is currently pretty low, and the anti-virus companies are creating signatures for the exploit and the related Trojans, worms, etc.

Second, consider the mitigation provided by your anti-virus, anti-spyware, host-based IDS, and any similar package. Even if the flaw exists, it is quite possible that the payload of any exploit will be snatched by the malware defense on the host. No one wants to have to rely on the last layer of “defense in depth” strategy, but that’s what the software is for.

Consider how many of these patches the organization is willing to install, even if all of them come from very reputable coders. The function exploited by this attack is probably not unique, there are possibly companion functions that will allow the same type of attack, certainly there are other file handling routines yet to be discovered as vulnerable to similar attacks.

If the patch is installed across an enterprise, what effect will that have on particular software support contracts? Even if problems are not related to WMF handling? At the least, a prudent enterprise will have to put more time into testing these patches than those released by Microsoft. Every organization will have to weigh all of these costs against the costs of infection.

Finally, it is a good time to close with a comment on the reality of being a security professional and risk manager. Every organization has varying thresholds of risk tolerance. Before acting, especially in a panic, weigh costs of action versus inaction. Will the lack of a patch result in 10 infections or 10,000? What is the policy for managing worm threats? If there is no strategy for tackling such emergencies (if one considers this an emergency), it is vital that one be established – and that prudence wins out when dealing with anything that management isn't ready for.

Update:

The first pieces of malware centered on this vulnerability a trickling in. One of the first is known as Nascene at Trend Micro's site. The attack comes by way of a "Happy New Year" greeting and attachment JPG file. Another entry is a mass-mailed Trojan, called Bankash.G by Symantec, which gathers passwords, account information, etc. from victim PCs.

References

Microsoft Security Bulletin MS05-053 – Vulnerabilities in Graphics Rendering Engine

<http://www.microsoft.com/technet/security/Bulletin/MS05-053.mspx>

CERT Notes on Vulnerability VU#181038

<http://www.kb.cert.org/vuls/id/181038>

Bankash.G

<http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.bankash.g.html>

NASCENE

<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FNASCENE%2EH>

Install Third-Party Patch to Thwart WMF Vulnerability

<http://isc.sans.org/diary.php?rss&storyid=996>

<http://www.f-secure.com/weblog/archives/archive-012006.html#00000760>

Guilfanov's Weblog

http://www.hexblog.com/2005/12/wmf_vuln.html